7710-12

This document is scheduled to be published in the Federal Register on 02/16/2022 and available online at **federalregister.gov/d/2022-03241**, and on **govinfo.gov**

POSTAL SERVICE

Privacy Act of 1974; System of Records

AGENCY: Postal Service™.

ACTION: Notice of a modified system of records.

SUMMARY: The United States Postal Service™.(USPS™) is proposing to modify a General Privacy Act System of Records to facilitate effective preparedness and response to potential emerging public health crises and other emergency events that may impact Postal Service employees and operations in the working environment.

DATES: These revisions will become effective without further notice on [INSERT DATE 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER] unless comments received on or before that date result in a contrary determination.

ADDRESSES: Comments may be submitted via email to the Privacy and Records Management Office, United States Postal Service Headquarters (privacy@usps.gov). Arrangements to view copies of any written comments received, to facilitate public inspection, will be made upon request.

FOR FURTHER INFORMATION CONTACT: Janine Castorina, Chief Privacy and Records Management Officer, Privacy and Records Management Office, 202-268-3069 or privacy@usps.gov.

SUPPLEMENTARY INFORMATION: This notice is in accordance with the Privacy Act requirement that agencies publish their systems of records in the Federal Register when there is a revision, change, or addition, or when the agency establishes a new system of records.

I. Background

The Postal Service has determined that General Privacy Act Systems of Records (SOR), USPS 500.300, Emergency Management Records, should be revised to facilitate effective preparedness and response to potential emerging public health crises and other emergency events that may impact Postal Service employees and operations in the working environment.

II. Rationale for Changes to USPS Privacy Act Systems of Records

The emergence of SARS-CoV-2 (COVID-19) in early 2020 identified the need for robust set of policies and practices to ensure operational continuity and employee safety amidst an emergency event, while also protecting individual privacy. To enhance the Postal Service's capability to respond to emergency events, the Postal Service will revise this SOR to broaden the scope of emergency events contemplated therein.

Further, this SOR will be revised to support the collection of information related to ongoing pathogenic public health crises, including an individual's inoculation status related to an ongoing pathogenic public health crisis, as well as to collect information on positive or negative diagnostic test results related to an ongoing pathogenic public health crisis.

These changes will provide greater flexibility to the Postal Service in its ability to prepare for and respond to a wide array of emergencies, and therefore provide greater support in its emergency management procedures.

III. Description of the Modified System of Records

The Postal Service will expand the types of Emergency events contemplated by this SOR, including:

- Natural disasters or other acts of God, such as coastal flooding, hurricanes, wildfires, etc.
- Manmade hazards, such as coastal oil spills and terrestrial chemical contamination.
- Manmade incidents, such as significant automobile accidents and active shooter events.
- Acts of international or domestic terrorism and impacts from terrorism, such as the September 11th, 2001 attacks on New York City; Arlington, Virginia; and Pennsylvania and the 1995 Oklahoma City Federal Building attack.
- Cybersecurity incidents, such as ransomware attacks and computer vulnerability exploits.
- Pathogenic public health crises, such as the Novel Coronavirus Disease-19 (COVID-19) pandemic and the 2014 Ebola outbreaks.

These events listed are intended as illustration and are not exhaustive of the types of events covered by the revisions to this SOR.

Additionally, this SOR has been revised as follows:

- Revisions to purposes 1,2, 4, and 6.
- Creation of purposes 7 through 13
- Revisions to Categories of Individuals 1 through 4
- Addition of Category of Individuals 5
- Revisions to Categories of Records 1,2, and 4
- Additions of Categories of Records 5 and 6
- Addition of Routine Uses b through e
- Revisions to Record Source Categories

Pursuant to 5 U.S.C. 552a (e)(11), interested persons are invited to submit written data, views, or arguments on this proposal. A report of the proposed revisions has been sent to Congress and to the Office of Management and Budget for their evaluations. The Postal Service does not expect this amended system of records to have any adverse effect on individual privacy rights. The notice for USPS 500.300, Emergency Management Records, provided below in its entirety, is as follows:

SYSTEM NAME AND NUMBER:

USPS 500.300, Emergency Management Records.

SECURITY CLASSIFICATION:

None.

SYSTEM LOCATION:

Headquarters and all field postal facilities.

SYSTEM MANAGER(S) AND ADDRESS:

Chief Postal Inspector, United States Postal Inspection Service, United States Postal Service, 475 L'Enfant Plaza SW, Washington, DC 20260.

Vice President, Organization Development, United States Postal Service, 475 L'Enfant Plaza SW, Washington, DC 20260.

Vice President, Facilities, United States Postal Service, 475 L'Enfant Plaza SW, Washington, DC

20260

Chief Information Security Officer Vice President, 475 L'Enfant Plaza SW, Washington, DC 20260

AUTHORITY FOR MAINTENANCE OF THE SYSTEM:

39 U.S.C. 401 and 410.

PURPOSE(S) OF THE SYSTEM:

1. To permit collaboration among officially designated individuals and agencies who are responsible for mitigation of, preparation for, response to, and recovery from any naturally occurring disaster, manmade hazard or incident, act of terrorism, cybersecurity incident, or pathogenic public health crisis, involving the Postal Service.

2. To satisfy federal requirements for the training, fitness testing, and medical surveillance of individuals in response to a naturally occurring disaster, manmade hazard or incident, act of terrorism, or pathogenic public health crisis, involving the Postal Service.

3. To test for the exposure of individuals to hazards.

4. To account for the whereabouts of individuals in response to a naturally occurring disaster, manmade hazard or incident, act of terrorism, or pathogenic public health crisis involving the Postal Service.

5. To assess the likelihood of an individual's exposure to a hazard and to contact the individual with important health-related information.

6. To provide information about disaster recovery programs and services to individuals affected by naturally occurring disaster, manmade hazard or incident, act of terrorism, or pathogenic public health crisis involving the Postal Service.

7. To track health evaluations, including temperature checks, self-reporting checklists, and laboratory tests related to an ongoing pathogenic public health crisis.

8. To utilize pathogenic public health crisis medical test results to provide contact tracing services to affected Postal Service employees, contractors, and customers.

9. To track and record vaccination status or employee attestation in lieu of acceptable proof of vaccination status as applicable, related to an ongoing pathogenic public health crisis, including the COVID-19 pandemic, to track and record pathogenic public health crisis medical test results, and maintain rosters with details relating to employees' vaccination status.

10. To provide limited personal information to relevant government health agencies for assistance tracking and controlling infections that are the subject of an ongoing pathogenic public health crisis.

11. To prepare for, identify, and respond to cybersecurity incidents aimed at or affecting the United States Federal Government or the Postal Service.

12. To allow an employee to record their COVID-19 vaccination status and COVID-19 testing status through mobile and web-based applications.

13. To allow an individual to upload their COVID-19 vaccination status and COVID-19 testing status to mobile and web-based applications by capturing an image of such status.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:

1. Postal Service employees, contractors, and other individuals having emergency management responsibilities officially designated by the Postal Service to mitigate, prepare for, respond to, or recover from any naturally occurring disaster, manmade hazard or incident, act of terrorism, pathogenic public health crisis, or cybersecurity incident.

2. Household members of Postal Service employees, contractors, and other individuals having emergency management responsibilities officially designated by the Postal Service to mitigate, prepare for, respond to, or recover from any naturally occurring disaster, manmade hazard or incident, act of terrorism, pathogenic public health crisis, or cybersecurity incident.

3. Individuals who are evacuees from postal facilities or who are unaccounted for in the event of a naturally occurring disaster, manmade hazard or incident, act of terrorism, or pathogenic public health crisis.

4. Individuals whose names have been provided to the Postal Service by government agencies or disaster relief organizations as a result of a naturally occurring disaster, manmade hazard or incident, act of terrorism, pathogenic public health crisis, or cybersecurity incident.

5. Postal Service employees who provide the Postal Service with acceptable proof of COVID-19 vaccination status or, in the alternative, weekly COVID-19 testing results (or test results prior to return to physical postal facilities or workplaces).

CATEGORIES OF RECORDS IN THE SYSTEM:

1. *Emergency management information:* Records related to Postal Service employees and contractors having officially designated emergency management responsibilities, including: name; Social Security Number or Employee Identification Number; date of birth; postal or contract assignment information; home, work, and emergency contact information; duty location, work schedule; and assigned emergency management devices.

2. *Medical fitness and surveillance information:* Records related to medical documentation such as: receipt of prophylaxis, a roster of COVID-19 vaccinations, other vaccinations, related to an ongoing pathogenic public health crisis, diagnostic tests, antibody tests, other medical tests as necessary and related to an ongoing pathogenic public health crisis, determinations of fitness to wear protective equipment, and surveillance for exposure to hazards.

3. *Emergency management training information:* Records related to specialized training in emergency management of natural disasters and manmade hazards completed by emergency management personnel.

4. *Evacuee information:* Records of individuals who are impacted by natural disasters or manmade hazards, such as name; postal or contract assignment information; home, work, and emergency contact information; home and work address; location in facility and activities prior to evacuation; route of exit from facility; rallying point; and emergency medical treatment administered to evacuees.

5. *Public Health Crisis Records*: Records of individual medical test results for infections relating to a state of emergency or public health crisis; records of individual vaccination against pathogens, a roster of employee vaccination status, identified as either fully vaccinated, partially (not fully) vaccinated, not fully vaccinated due to a medical or religious accommodation, non-disclosed, or vaccine attestation statements provided in lieu of proof of vaccination; and reports of work-related COVID-19 fatalities and work-related COVID-19 in-patient hospitalizations.

6. *COVID-19 Software Application Records*: Employee Identification Number, Vaccination Status, Vaccine Manufacturer, Vaccine Date, Postal Email Address, Personal Email Address, Vaccine Proof Image, Vaccine Exemption Status, Vaccine Exemption Reason, Test Result Status, Last Testing Date, Testing Kit Result Image, Date of Test, and Attachment Uploads.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

Standard routine uses 1 through 9 apply. In addition:

a) Medical records may be disclosed to an individual's private treating physician, to medical personnel retained by the Postal Service, and to public health agencies to provide medical examinations, medications, or treatment to individuals covered by this system of records.

b) Personal information, not to exceed name, positive or negative pathogenic public health crisis diagnostic test results, testing facility name, testing facility contact information, positive or negative pathogenic public health crisis antibody test results, address, and preferred contact information, may be disclosed to the Centers for Disease Control and Prevention, National Institutes of Health, and any relevant state or local public health authorities covering an area affected by an ongoing pathogenic public health crisis.

c) Disclosure of records to appropriate agencies, entities, and persons when (1) the Postal Service suspects or has confirmed that there has been a breach of the system of records; (2) the Postal Service has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, the Postal Service (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Postal Service's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

d) Disclosure of employee COVID-19 vaccine documentation and any COVID-19 test results to the Assistant Secretary of Labor for Occupational Safety and Health, their designees, employees, individuals authorized by that employee, or employee representatives upon request.

e) Disclosure of work-related COVID-19 fatalities and hospitalizations to the Occupational Safety and Health Administration (OSHA).

RECORD SOURCE CATEGORIES:

Employees; contractors; medical staff of the Postal Service; designated contractors; public health agencies; emergency response providers, first responders; individuals who are evacuated in the event of a naturally occurring disaster, manmade hazard or incident, act of terrorism, pathogenic public health crisis, or cybersecurity incident; and household members of USPS employees and other individuals having emergency management responsibilities officially designated by the Postal Service.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS:

Automated database, computer storage media, and paper.

POLICIES OF PRACTICES FOR RETRIEVAL OF RECORDS:

By name, Social Security Number, Employee Identification Number, and postal facility name.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

- Emergency management information and emergency management training information is retained 5 years beyond the end of the period for which the individual is assigned emergency management responsibilities.
- Medical documentation including fitness and medical surveillance information is retained 30 years from the date of collection.
- Evacuee information is retained 5 years from the date of collection.
- Records related to employee vaccination and employee medical test related to a pathogenic public health crisis are retained for 5 years from date of collection.
- Records related to COVID-19 Software Application Records are retained for 24 months.

Records existing on paper are destroyed by burning, pulping, or shredding. Records existing on computer storage media are destroyed according to the applicable Postal Service media sanitization practice.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:

Paper records, computers, and computer storage media are located in controlled-access areas under supervision of program personnel. Access to these areas is limited to authorized personnel, who must be identified with a badge. Access to records is limited to individuals whose official duties require such access. Contractors and licensees are subject to contract controls and unannounced on-site audits and inspections. Computers are protected by mechanical locks, card key systems, or other physical access control methods. The use of computer systems is regulated with installed security software, computer logon identifications, and operating system controls including access controls, terminal and transaction logging, and file management software.

RECORD ACCESS PROCEDURES:

Requests for access must be made in accordance with the Notification Procedure above and USPS Privacy Act regulations regarding access to records and verification of identity under 39 CFR 266.5.

CONTESTING RECORD PROCEDURES:

See Notification Procedure (below) and Record Access Procedures (above).

NOTIFICATION PROCEDURE:

Current and former employees and contractors wanting to know if information about them is maintained in this system of records must address inquiries to the facility head where currently or last employed. Headquarters employees or contractors must submit inquiries to the Chief Postal Inspector. Requests must include full name, Social Security Number or Employee Identification Number, and employment or contract dates. Individuals from whom evacuee information may have been collected must address inquiries to the head of the facility from which they were evacuated. Household members of current or former field employees and other individuals having emergency management responsibilities officially designated by the Postal Service must address inquiries to the facility head where the postal employee in their household is currently or was last employed. Household members of current or former Headquarters employees and other individuals having emergency management responsibilities officially designated by the Postal Service must submit inquiries to the Chief Postal Inspector.

SYSTEMS EXEMPTED FROM CERTAIN PROVISIONS OF THE ACT:

Pursuant to 5 U.S.C. 552a(j) and (k), USPS has established regulations at 39 CFR 266.9 that exempt records in this system depending on their purpose.

HISTORY:

June 27, 2012, 77 FR 3834; July 17, 2008, 73 FR 41134; April 29, 2005, 70 FR 22516

Sarah E. Sullivan,
Attorney, Ethics & Legal Compliance.

[FR Doc. 2022-03241 Filed: 2/15/2022 8:45 am; Publication Date: 2/16/2022]